# Table of Contents

## F01 System Functions

**Subject** **Page**




Initial Print Date: 01/09 Revision Date:

**Subject** **Page**

BLANK
PAGE

# System Functions

## Model: F01/F02

## Production: From Start of Production

# OBJECTIVES

After completion of this module you will be able to:

- Explain the method in which diagnostic data is captured by the control units
- Identify the components in the system where data is centrally stored
- Identify and explain the various modes of operation for the control units
- Explain the purpose and operation of the ethernet connection on the vehicle
- Explain Sweeping technology
- Explain the process necessary for updating navigation map data
- Identify and explain the need for increased security features for the data in the vehicle

# Diagnostics Master

The Diagnostics Master function is a function distributed throughout the vehicle. It is divided into the following subfunctions:

- Time Master
  Includes the centralized specification of a system time for all control units in the vehicle, and the application as a time stamp for fault messages from control units.
- Centralized fault memory
  Includes the saving of fault and Check Control messages with centralized ambient conditions.
- Specification of the fault memory status
  Includes the centralized specification a fault memory block for network fault memory entries in specific situations as well as the evaluation/application of the block in the client control units.

One task is often divided over multiple computers in a computer network (this also includes control units with bus connections). It is important to specify the computer (or control unit) that has the main function. This control unit is then described as the main control unit or "master". All other computers (control units) are called “peripherals” or "secondary controllers".

Each subfunction of the diagnostics master includes a master portion and a secondary portion. The master portion is always implemented in a single control unit, but the secondary controller portion in all participating control units.

| Subfunction | Master |
|---|---|
| Time master | KOMBI |
| Centralized storage of fault messages | ZGM |
| Specification of the fault memory status | Junction Box |

## Time Master

The Time Master is located in the instrument panel and cyclically transmits the system time to all other control units in the vehicle every second.

This system time is set to zero only once in the life cycle of the vehicle while in the factory at the end of the production process. The system time expresses the time in seconds that have passed since initialization in the factory.

The counter for the system time is not reset when the battery is disconnected or when the power to the instrument panel is switched off.

When the battery is disconnected the time value is actually initially lost, but it is updated when the power supply is again available. This is achieved by reading the last value stored in the non-volatile memory (EEPROM), increasing it by one time unit, and applying it in the Time Master as a new system time. The counter for the system time can map a time of approximately 136 years.

The system time is received by all control units, and used it as a time stamp when fault messages are stored.

To allow retention of the system time even after replacement of the instrument panel, it is stored redundantly in the CAS similar to the mileage reading.

## Centralized Fault Memory

This subfunction has the task of centralized storage of fault and Check Control messages in addition to the local fault memories for each of the control units and the storage of CC messages in the instrument panel. The central gateway module (ZGM) is the master for this function and it is also called the Diagnostics Master.

Whenever faults occur, all control units locally save the fault along with at least the two mandatory environmental conditions of kilometer reading and system time. A new function is that the control units additionally signal the fault code and the system time at which the fault occurred (time stamp) to the Diagnostics Master (ZGM).

The fault memory concept and fault memory process of the control units have not been changed by the additional reporting to the Diagnostics Master. This means a control unit "very normally" makes a self-defined fault memory entry. The local fault memory entry remains untouched in the local fault memory of the secondary control unit.

The Diagnostics Master then additionally centrally stores the fault code and a fixed set of 26 ambient conditions at the same time that it indicated in the time stamp.

The ambient conditions stored on the fault message by the Diagnostics Master include different information on the global status of the vehicle such as the:

- Standard time
- Vehicle system voltage
- Outside temperature
- Terminal status
- Kilometer reading
- Vehicle driving speed

The central fault memory in the ZGM has a size of 18 kB. Between 250 and 1000 fault events and Check Control messages can be stored centrally in the ZGM dependent upon how many faults occur simultaneously. When the fault memory is full no new faults or Check Control messages are stored. The fault and Check Control messages in the central fault memory can then only be deleted via the BMW diagnostic system.

Each fault code and each Check Control message is accepted up to 10 times. Without this limit, a constantly occurring fault would very quickly fill the entire central fault memory.

These ten entries are sufficient for analysis of the fault.

All central fault memory entries are lost when the ZGM is replaced.

**Note: Primary fault analysis continues to be performed by using the fault memory entries in each of the control units. The data from the central fault memory of the Diagnostics Master serve to supplement and allow a more precise diagnosis. Functions for using this data are integrated in the new workshop system.**

Advantages:

Previously (without Diagnostics Master), only the kilometer reading and system time (mandatory environmental conditions) and possibly a few additional ambient conditions could be found in the local fault memories.

The ZGM stores 26 additional ambient data items for each fault memory entry from each of the control units.

Additionally, up to 10 time instances at which the fault occurred are recorded in the ZGM for a fault code.

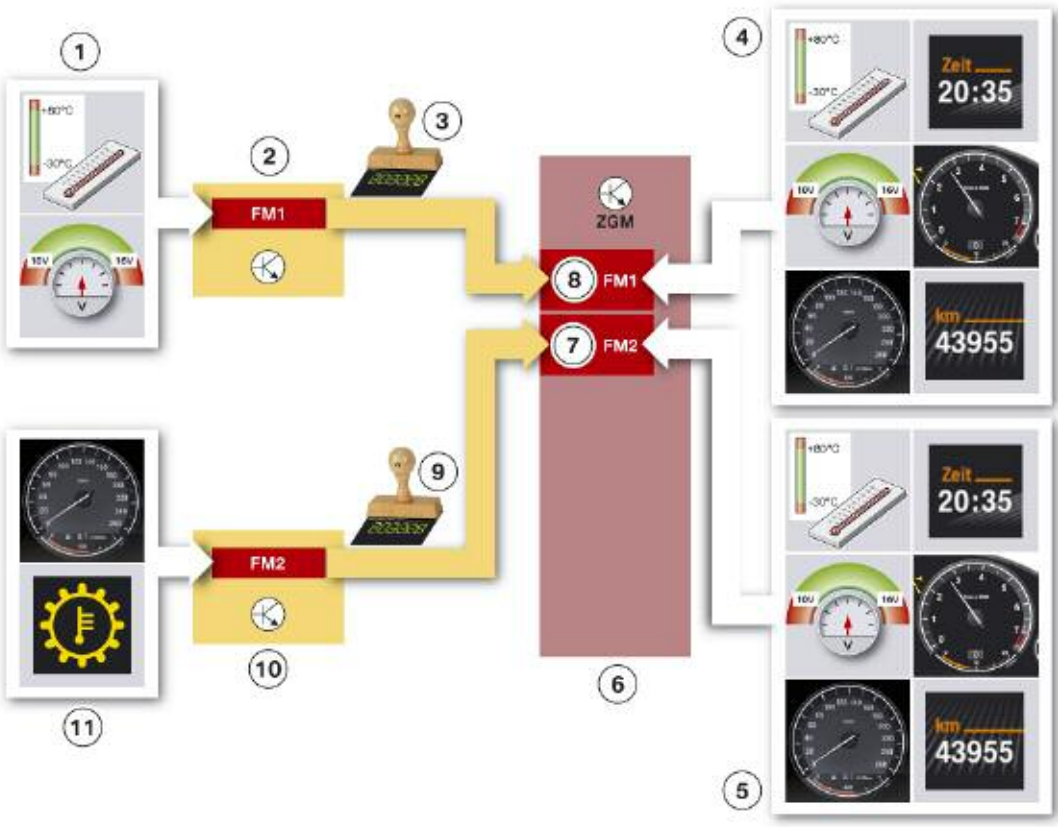
The time stamp with second-precision permits a statement upon the time sequence of fault events, which was previously not possible based solely upon the kilometer reading. For the first time it is possible to the name the cause and effect with greater clarity for distributed functions, e.g. the control unit that firstly entered a fault, the control unit that in consequence only entered a fault as a reaction, etc.

The Check Control messages at the time of the fault are also stored in the Diagnostics Master and are also provided with the 26 ambient conditions. "Customer complaints" can be assigned better to a vehicle situation because of the Check Control messages and above all also corresponding fault memory entries.

These measures have made a more precise diagnosis possible.

**Note: Up to 55 fault codes (also without time stamp or ambient conditions as is currently the case) can still be stored In the CAS and in the identification sensor of the F01/F02.**

## Storage of faults in the F01/F02




| Index | Explanation | Index | Explanation |
|---|---|---|---|
| 1 | Two local ambient conditions for fault 1 | 7 | Fault message 2 (FM2) |
| 2 | Fault 1 and 2 local ambient conditions are stored in the fault memory of the control unit | 8 | Fault message 1 (FM1) |
| 3 | Fault message 1 (FM1) and the "time stamp" are sent to the Diagnostics Master | 9 | Fault message 2 (FM2) and the "time stamp" are sent to the Diagnostics Master |
| 4 | Central ambient conditions at the time when fault 1 occurred | 10 | Fault 2 and 2 local ambient conditions are stored in the fault memory of the control unit |
| 5 | Ambient conditions at the time when fault 2 occurred | 11 | Two local ambient conditions for fault |
| 6 | Diagnostics Master in the ZGM | | |

## Specification of the Fault Memory Status (pseudo fault reduction)

In certain vehicle operating situations invalid fault memory entries (pseudo faults) are made as the control units do not behave synchronously in these situations. The critical operating situations occur during:

- Wake-up of the vehicle
- Start of the combustion engine
- Under/Overvoltage

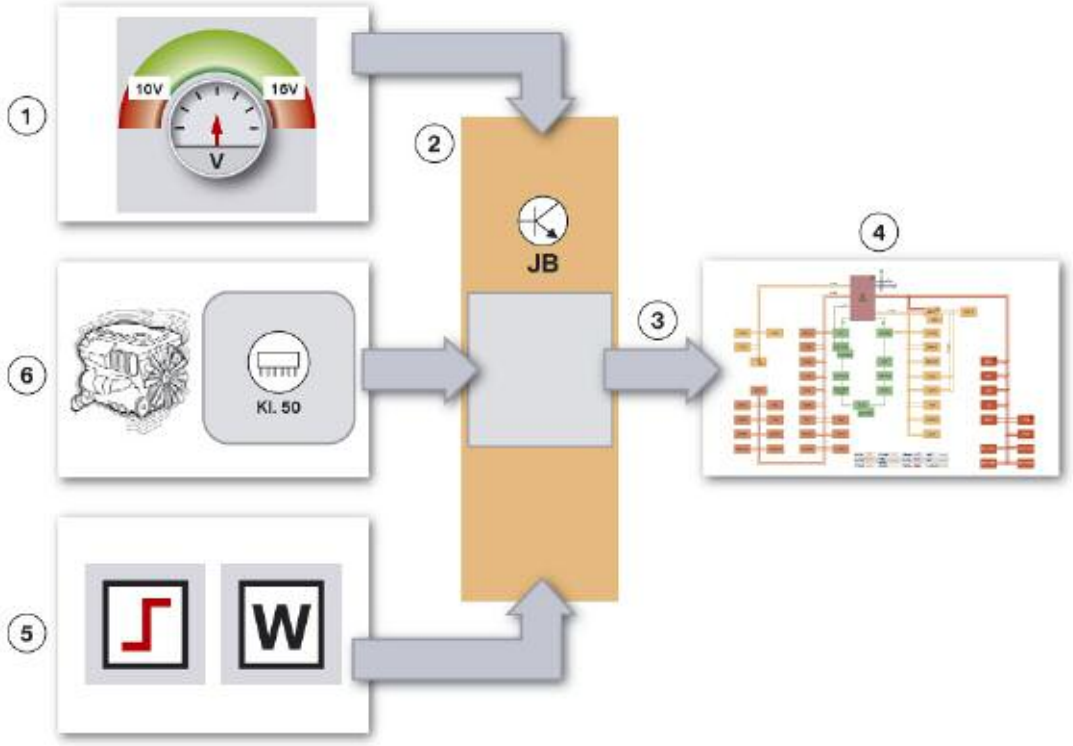
To prevent pseudo faults in these operating situations, a centrally communicated signal forbids specific faults from being entered in the local fault memories of the control units.

These will simultaneously actively prevent these faults being signalled to the master of the "storage system context" function and from being entered in the central fault memory.

The fault memory block is not only effective for network fault memory entries, however not for control units-fault memory entries.

The fault memory entries for control units relevant for exhaust gas and safety are not affected by this function and they will always be written.

## Saving of faults is prevented under certain circumstances




| Index | Explanation |
|---|---|
| 1 | Under/Overvoltage<br>block condition: 10.5 V < U < 16 V<br>Unblock condition: U > 11 V or U < 15.5 V |
| 2 | Junction Box (master for the subfunction specification of fault memory status) |
| 3 | Bus message "status - block fault memory" |
| 4 | All control units |
| 5 | Wake-up of the vehicle<br>Block condition: wake-up signal<br>Unblock condition: three seconds after wake-up signal tw > 3 s |
| 6 | Engine start (Terminal 50) block condition: Terminal 50 active |

# Vehicle Status Management

Vehicle status management is a system function with the task of implementing standardized system behavior in different operating conditions for all future BMW vehicles.

For instance, the different switch-on behavior of the radio. To switch on the radio in the E65, the START-STOP button must be pressed (Terminal R is switched on). In the E90, on the other hand, the radio can also be switched on without inserting the key's remote control into the insertion slot.

The vehicle status management system calculates a single vehicle status from the terminal status, vehicle movement, battery condition and status of the combustion engine. This status is then used to define when a customer function or a group of customer functions (e.g. all entertainment functions) has to be available.

Furthermore, the vehicle status management system controls the operating mode the vehicle or specific modules are in. Those functions that are to be available in a mode are controlled.

*Example:* No radio operation while in the transportation mode.

Distinction is drawn between the following operating states:

- Standby
- Basic control mode
- Ready to drive
- Engine start
- Driving

A further vehicle status management task is the simultaneous start up and shut down of the on-board communication network.

**F01 on the production line**

## Start up and Shut Down of the Onboard Communication Network

The vehicle status management system describes the start up and shut down of the onboard communication network. In addition to general requirements, that are binding for all control units, the cascading, wake-up and sleep memories are defined.

### Cascading

The cascading function ensures that all buses in the vehicle electrical and bus systems startup in coordination and shut down or "sleep" simultaneously. This function is made possible by a master function of the central gateway module (ZGM) that specifies whether the vehicle electrical and bus systems may sleep. This master function controls the secondary control units, each of which is responsible for the start-up and sleep for one bus. Secondary controllers are located in the following control units:

- ZGM (for K-CAN, K-CAN2, PTCAN, FlexRay and MOST)
- DME (for the PT-CAN2)

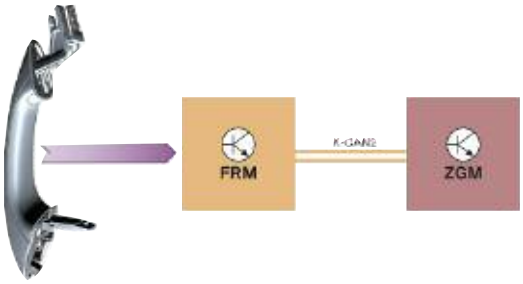
### Wake-up and Sleep Memory

In the event that the vehicle should not correctly wake-up or sleep, this often results in an increased power requirement for the complete vehicle, which may cause an empty battery and therefore a broken-down vehicle.

With the wake-up and sleep memory, the vehicle status management makes functions available for detection of faulty wake-up and sleep processes and initiation of countermeasures. For this purpose, the vehicle status management system has firstly recorded all possible reasons that could allow a control unit to wake-up the vehicle. When such a reason exists, the waking control unit must signal this reason to the wake-up and sleep memory that is contained in the ZGM.

Should a faulty wake-up exist, it is logged in the ZGM (fault memory entry that includes also the waking control unit and the wake-up reason as ambient conditions). The time and current kilometer reading are always saved as further ambient conditions. In this instance, the ZGM initiates countermeasures by transmitting the diagnostic command "powerdown". Should faulty wake-up events continue to occur after this, a reset of terminal 30F and then a permanent switch-off of terminal 30F is required. Just as with wake-up, faults may also occur for sleep. For such a fault, the wake-up and sleep memory creates a fault memory entry and initiates the same measures as for faulty wake-up.

All control units that may wake-up the vehicle are defined and assigned an identification number (hexadecimal number). Two seconds after each control unit has completed the wake-up process it transmits the bus message "wake-up registration FZM" to the ZGM and notifies the reason for the wake-up.




*Example:*

Wake-up by opening the driver's door FRM transmits the following message two seconds after the wake-up:

- Message ID: 0x5F2 (identification number for FRM)
- Byte 0: 0x27 (bus message "wake-up registration FZM")
- Byte 1: 0x72 (identification number FRM)
- Byte 2: 0x10 (Wake-up cause "door contact, front left")

**Wake-up of the Vehicle**

The bus overview of the F01/F02 with wake-authorized and wake-capable control units is shown below.

Wake-authorized control units may wake-up the vehicle electrical and bus systems.


The wake-authorized control units are shown on the bus diagram on the following page by a rising-edge symbol.

The wake-authorized control units include:

- K-CAN2: FRM, FZD, JB,
- K-CAN: IHKA
- MOST: RSE High, ULF-SBX High, ULFSBX and TCU

Wake-capable control units are woken up via a wake-up line.

The wake-capable control units are identified with a "W". These control units are woken up via a wake-up line.

These include:

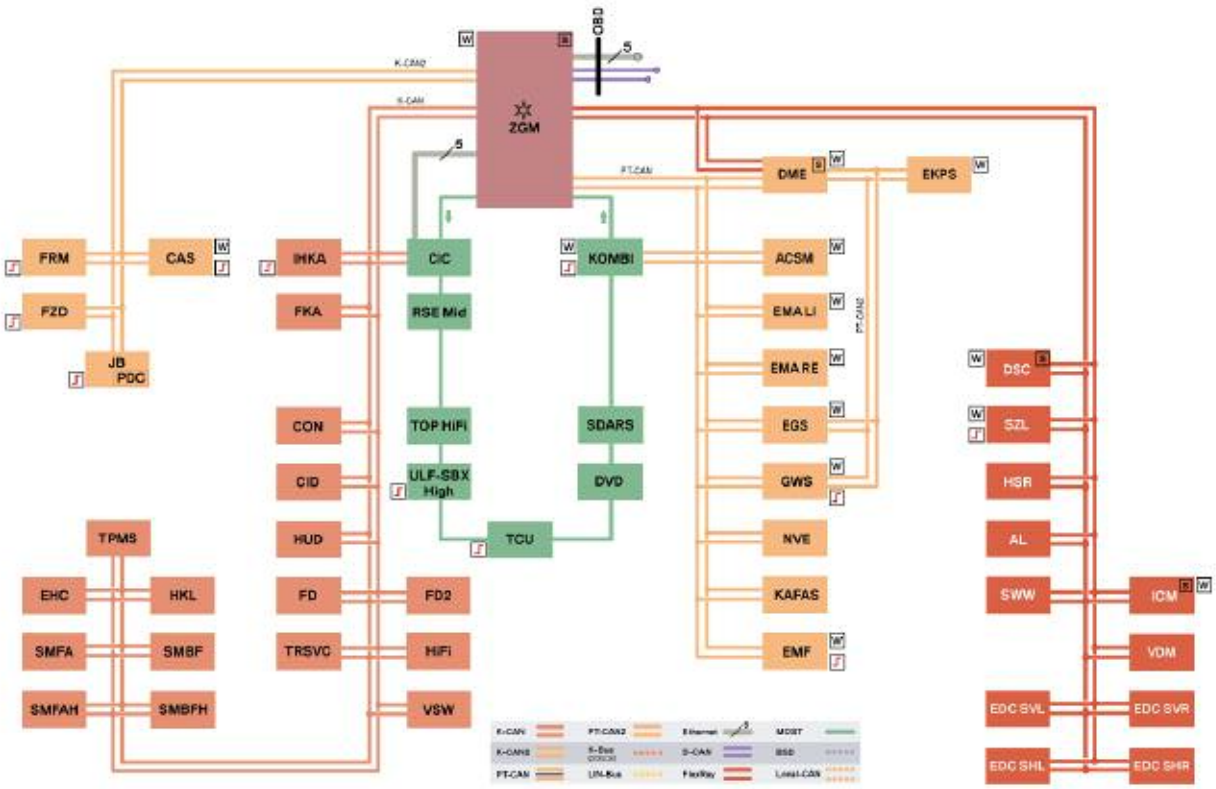
- ZGM
- PT-CAN: DME, ACSM, EMA LI, EMA RE, EGS
- FlexRay: DSC and ICM

Additionally, there is a group of control units that are “wake-authorized” as well as wake capable:

- K-CAN2: CAS
- MOST: Kombi
- PT-CAN: GWS and EMF
- FlexRay: SZL

The remaining control units are then woken up via the bus systems or via switching on the power supply.

## Bus overview F01/F02 with wake-authorized/capable control units




| Index | Explanation | Index | Explanation |
|---|---|---|---|
| ACSM | Advanced Crash Safety Module | DVD | Digital Video Disc |
| AL | Active Steering | EDC SHL | Electronic Damping Control (Satellite rear left) |
| CAS | Car Access System (CAS 4) | EDC SHR | Electronic Damping Control (Satellite rear right) |
| CIC | Car Information Computer | EDC SVL | Electronic Damping Control (Satellite front left) |
| CID | Central Information Display | EDC SVR | Electronic Damping Control (Satellite front right) |
| CON | Controller | EGS | Electronic Transmission Control |
| DME | Digital Motor Electronics | EHC | Electronic Height Control |
| DSC | Dynamic Stability Control | EKPS | Electric Fuel Pump |

| Index | Explanation | Index | Explanation |
|---|---|---|---|
| EMA LI | Electrically motorized reel, left | NVE | Night Vision Electronics |
| EMA RE | Electrically motorized reel, right | PDC | Park Distance Control |
| EMF | Electromechanical Parking Brake | OBD | On Board Diagnostic Connector |
| FD | Rear Display, left | RSE | Rear Seat Entertainment (Mid) |
| FD2 | Rear Display 2, right | SDARS | Satellite Radio |
| FKA | Rear compartment, heating/air conditioning | SMBF | Seat module, passenger |
| FLA | High Beam Assistant | SMBFH | Seat module, passenger rear |
| FRM | Footwell Module | SMFA | Seat module, driver |
| FZD | Roof Functions Center | SMFAH | Seat module, driver side rear |
| GWS | Gear Selector Lever | SWW | Lane Change Warning (Active Blind Spot Detection) |
| HiFi | HiFi Amplifier | SZL | Steering column switch cluster |
| HKL | Trunk Lid lift | TCU | Telematics Control Unit |
| HSR | Rear axle drift angle control (Rear Steering Control Module) | TOP-HIFI | TOP-HiFi Amplifier |
| HUD | Head-up Display | TPMS | Tire Pressure Monitoring System |
| ICM | Integrated Chassis Management | TRSVC | Top Rear Side View Camera Module for rear/side view cam |
| IHKA | Integrated Heating and Air Conditioning, automatic | ULF-SBX High | Interface Box, high version |
| JB | Junction Box Electronics | VDM | Vertical Dynamics Management |
| KAFAS | Camera-assisted Driver Assistance Systems | VSW | Video Switch |
| KOMBI | Instrument Cluster | ZGM | Central Gateway Module |

## Calculation of the Vehicle Status and Control of Vehicle Functions

The vehicle status management system calculates a single vehicle status from the terminal status, vehicle movement, battery condition and status of the combustion engine. This status is then used to describe when a customer function or a group of customer functions (e.g. all entertainment functions) has to be available.

For instance, all functions for geometric adaptation are to be available in the basic control mode/stationary operation statuses. The operating states defined through vehicle status management are summarized in the following table:

| Operating State | Identifying Feature | Function |
|---|---|---|
| Driving | Engine running | Active steering |
| Engine start | Starter motor running | Radio mute |
| Ready to drive | Engine OFF, driver present, ignition switched ON | This is where those functions are activated that are required for the driving mode, e.g. Park Distance Control, air-conditioning system, passive safety systems |
| Basic control mode | Engine OFF, driver present, ignition switched OFF | Radio, seat adjustment |
| Standby | Driver's absence identified by:<br>• Secure vehicle, or<br>• Non-initiation of driver interaction for 30 minutes. | Functions that have to exist when the driver is absent, e.g. DWA, CAS (read-in remote control) |

## Control of Operating Modes

Those functions that are to be available in an operating mode are defined (e.g. no radio operation in transportation mode) via the vehicle status management system. There are three operating modes: manufacture, transportation, flash, which are abbreviated in German as FeTraFla mode.

FeTraFla mode replaces the former manufacture, transportation, workshop or FeTraWe mode. Workshop mode has rarely been used to date and has been replaced by flash mode.

Flash mode offers the advantage that communication between the control units is reduced to a minimum during programming, and therefore higher data transfer rates are achieved from the BMW Programming system into the vehicle. Additionally, the control units are notified that programming is taking place.

This prevents the control units from going into emergency operation (e.g. the windscreen wiper does not start).

Flash mode is activated via a diagnostic command. The control units permanently save this mode. This has the advantage that the control units still know that they are in flash mode after a reset. In earlier vehicles a reset often had the consequence that a control unit had interrupted communication and this had consequently caused a flash termination.

It is also possible to use the "extended operating modes" to further subdivide a mode in order, for instance, to suppress or activate functions only at specific conveyor belt sections during manufacture.

# Ethernet Access

The increasing number and complexity of functions in the vehicle cause a constantly increasing rise in the number of control units and consequently the data volume in the vehicle. When these data are to be updated the vehicles must be programmed over the BMW programming system. The number of BMW vehicles that can be programmed has constantly increased since the introduction of the E65 in 2001.

The challenge facing the Service Department is the programming of ever increasing data in increasing numbers of vehicles.

In order to accelerate the programming procedure in the workshop, an Ethernet access has been integrated in the diagnostic socket of the F01/F02 in addition to the OBD access (D-CAN).

It is Fast Ethernet compliant with IEE802.3 2005 100 base TX.

This standardized interface provides a centralized, standardized access in the vehicle. This access permits IP-based communication with the vehicle.

The vehicle is therefore uniquely identifiable as a communication partner in an IP-based network, and BMW diagnosis and programming systems can be used in the workshop for the data exchange with the vehicle.

**Note: The previously used MOST direct access is not installed in the F01/F02.**

## What is Ethernet?

Ethernet is a cabled data network technology for local area networks (LANs). It facilitates the data exchange in the form of data frames between all devices (computers, printers, etc.) connected in a local network (LAN). Earlier the LAN only extended over one building.

Today the Ethernet technology uses fiber glass or radio to also connect devices over long distances.

Ethernet was invented over 30 years ago. A protocol was used as a transmission protocol that was in use at that time for radio-based networks.

Consequently the name Ether, that had been assumed historically to be the medium for propagation of radio waves.

In an Ethernet network, the users in the common cable network transmit messages via high-frequency signals.

Each network user has a unique 48-bit key that is called the MAC address. This ensures that all systems in an Ethernet have different addresses.

MAC is an acronym for Media Access Control.

The MAC address is required because a commonly used medium (network) can not be used simultaneously by multiple computers without data collisions, and therefore communication faults or data losses occur in the short or long term.

Different data transfer speeds were defined during development of Ethernet. Since 1995 the 100 Mbits/s standard has been used and it is called Fast Ethernet.

In the F01/F02, Fast Ethernet compliant with standard IEEE 802.3 2005 100 base TX with 100 Mbits/s data transfer rate is used.

100 Mbit/s Ethernet is also used today as the LAN connection for PCs.

**Ethernet connection for a PC**

In addition to a higher data rate, the 100 Mbits/s Ethernet offers the following advantages:

- All BMW dealers have an Ethernet infrastructure
- Ethernet is future-proof
- Standard IT technologies can be used inside and outside of the vehicle
- Ethernet allows a cable length of 100 m (cable length today in workshop = 10 m)

## Ethernet Port

As there were enough free pins in the diagnostic socket it was possible to integrate the Ethernet port in this socket.

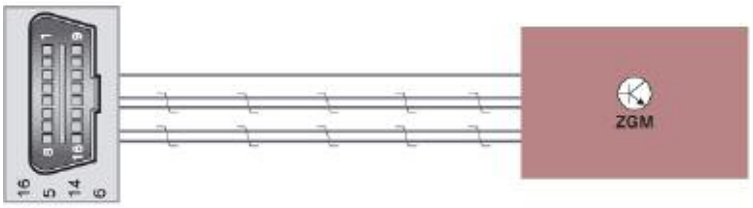
This installation location is the optimal solution for the vehicle access. The further advantage lies in that D-CAN as well as Ethernet can be connected to BMW diagnostic and programming systems via one connection (ICOM A).

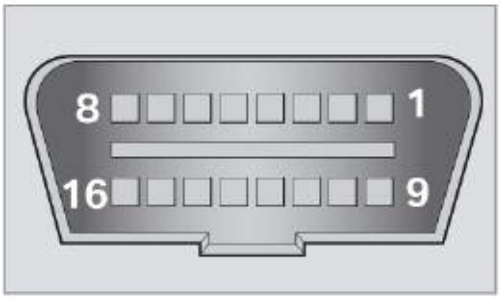
Five pins are used for the Ethernet port in the diagnostic socket.

These five lines are routed from the diagnostic socket to the central gateway module (ZGM).

One of the five lines transmits the activation signal. The remaining four lines are twisted pair and are used for data transmission.

**Ethernet connection between the diagnostic socket and ZGM**






| Index | Explanation | Index | Explanation |
|---|---|---|---|
| 1 | Not assigned | 9 | Engine speed |
| 2 | Not assigned | 10 | Not assigned |
| 3 | Ethernet Rx+ | 11 | Ethernet Rx- |
| 4 | Terminal 31 | 12 | Ethernet Tx+ |
| 5 | Terminal 31 | 13 | Ethernet Tx- |
| 6 | D-CAN High | 14 | D-CAN Low |
| 7 | Not assigned | 15 | Not assigned |
| 8 | Ethernet activation | 16 | Terminal 30F |

## Activation of the Ethernet Access

The Ethernet access is switched off in normal operation. It must be activated prior to every usage and then deactivated after it has been used.

Upon connection of the ICOM A, the activation line (Pin 8) is connected to terminal 30B (Pin 16) and this activates the Ethernet access.

The Ethernet module in the ZGM receives the signal (voltage level of terminal 30B) via the activation line. When the ICOM A is disconnected from the diagnostic socket the Ethernet access is deactivated. When the customer is in driving mode the Ethernet access is always deactivated.

Each user in an Ethernet is assigned an identification number that is unique throughout the world, the MAC address (Media Access Control). A user in a network is uniquely identifiable via the MAC address. The MAC address of the vehicle is located in the ZGM and can not be changed.

The VIN (Vehicle Identification Number) identifies the vehicle to the BMW programming system. Before communication with the vehicle can take place, just the same as for a computer network in the office it is necessary for each device in an IP-based network to have received a logical identification, called the IP address. The IP address is only unique in the respective network segment (subnetwork) and it can be assigned dynamically or statically.

After activation of the Ethernet connection and establishment of the physical connection the central gateway module is assigned the IP address from the ICOM A. Through a special process, the so-called "vehicle identification", the IP address, VIN and MAC are exchanged between the BMW diagnosis or programming systems and the ZGM. This allows unique identification of the vehicle in the workshop network and therefore a communication connection can also be established.

The function of an IP address in a network corresponds to a phone number in the telephone network. Assignment of this IP address is performed per DHCP (Dynamic Host Configuration Protocol). This is a process for automatic allocation of IP addresses to new end devices in a network. Merely the automatic reference to IP address must be set on the end device.

It must be possible to assign the IP address dynamically (DHCP server) for operation in a changing workshop network infrastructure.

The vehicle should adapt to the network and not the network to the vehicle. After disconnection of the ICOM A the assigned IP address is released upon expiry of the time set in the DHCP server.

Data enters into the vehicle and is distributed in the vehicle via the Ethernet access over the central gateway module.

The Ethernet connection does not have any effect upon the operation and time response of the D-CAN connection.

**Note: Simultaneous operation of the D-CAN and Ethernet access must be prevented, as this makes collisions of diagnostics commands within the vehicle probable and therefore communication via both accesses can become faulty.**

## Vehicle Connection to the BMW Shop Network

An example of connection of the F01/F02 to the BMW workshop network is shown in the diagram below.

An IP address is automatically assigned to the vehicle after connection of the ICOM A. This allows unique identification of the vehicle (the ZGM) in the BMW workshop network, and a communication connection is established.

Authentication must be completed, and a signature is necessary for writing (programming) data into the vehicle. As opposed to this, it is possible to read (diagnosis) data

immediately after a data line has been connected to the vehicle. The authentication and signature prevent third parties from changing data records and memory values.

Programming is carried out using the Software Service Station and ISTA-P.

The ICOM A must always be connected to the workshop network over LAN cable to allow programming to be carried out.

Programming is always performed over the Ethernet access. Only the diagnosis and no programming is performed over D-CAN.

The connection to the vehicle must be retained until programming has been fully completed. The ZGM assumes the gateway function and distributes data over the buses to the other control units.

## Definitions

**Authentication**
Authentic from the Greek work "authentikos" = valid, real, credible.

Authentication = confirmation of authenticity

To authenticate = to make valid, make credible.

Nowadays the conformation of authenticity is often stated in connection with rights of use e.g. for PCs or access to buildings.

**Authentification**
The process of proving the identity (authenticity) upon request.

For instance, check of the user password by the PC system.

An example to clarify authentification, authentication and authorization:

A user wants to log on to his PC. He authenticates himself.

The PC system wants to check whether the user is entitled to log on to the system: It authentifies.

After it has completed the check, the PC grants access: It authorizes the user.

**Digital Signature**
= Digital acceptance

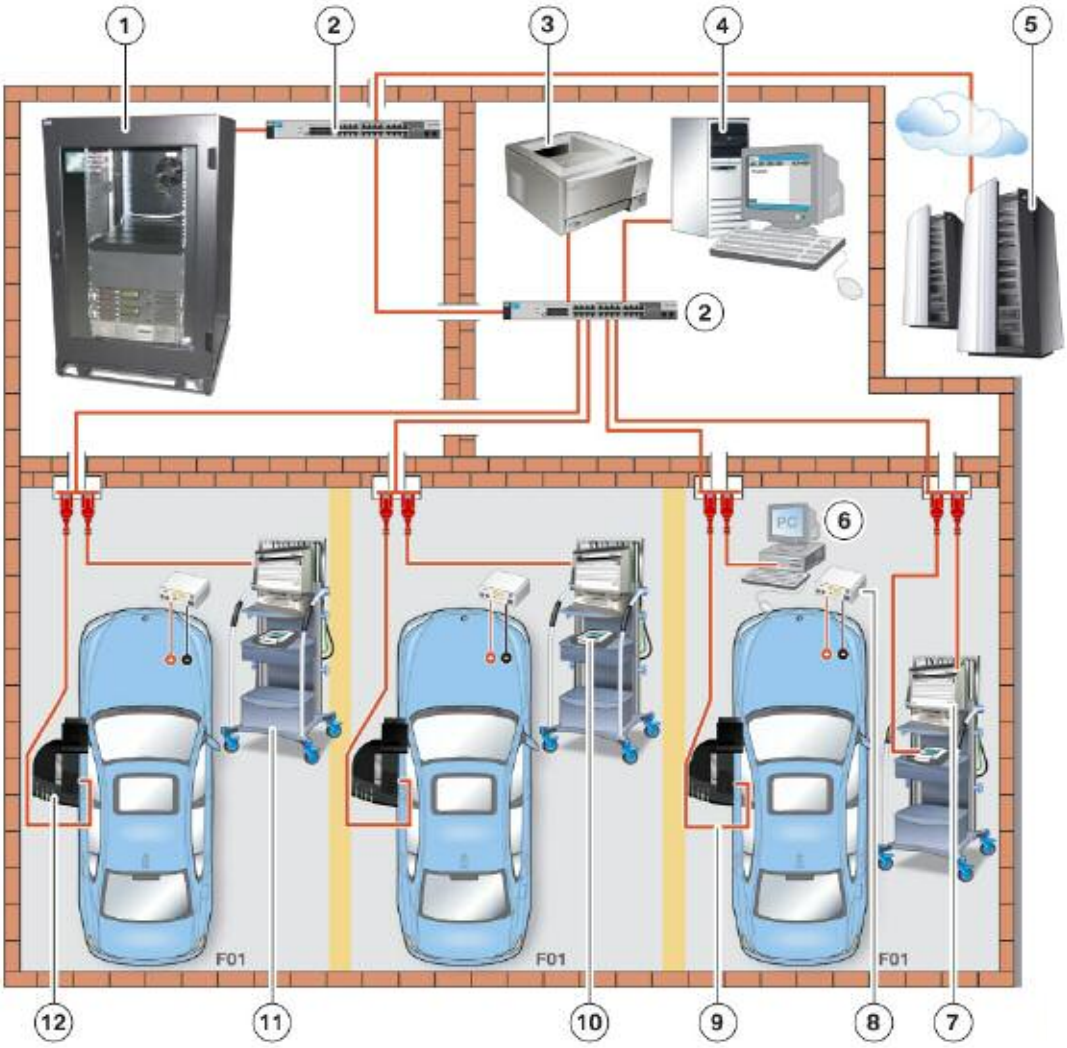
From the Latin "Signum" the sign.

A digital signature in an encryption procedure with the purpose of ensuring the trustworthiness of a person.

In this case, the authorship and affiliation of data to a specific person is checked.

Simultaneously the completeness, genuineness and intactness of the signed electronic data are checked.

## Vehicle Connection to the BMW Shop Network




| Index | Explanation | Index | Explanation |
|---|---|---|---|
| 1 | Integrated Service Information Server (ISIS1) | 7 | Integrated Service Information Display (ISID) |
| 2 | Gigabit switch | 8 | Battery charger |
| 3 | Printer | 9 | LAN cable |
| 4 | Integrated Software Service Station (ISSS) | 10 | Integrated Measurement Interface Box (IMIB) |
| 5 | BMW Group server | 11 | Workshop trolley |
| 6 | Workshop PC | 12 | Integrated Communication Optical Module (ICOM A) |

# Vehicle Configuration Management

The vehicle configuration management system (VCM) is a system function and has the primary task of centralized storage of data structures in the vehicle. The VCM integrated in the central gateway module ZGM as a system function.

The vehicle order and the I-levels in addition to the security are stored in the CAS. This ensures that the information can be restored after the ZGM has been replaced. The information stored in the vehicle configuration management system can be called by diagnostic commands upon request from the diagnosis system or internal vehicle system functions.

This means that the current vehicle configuration is saved centrally at precisely one place and a consistent information status is assured. This configuration knowledge only needs to be maintained at only one place. As this information is stored in the vehicle it is available at all times to all systems outside of the vehicle (diagnosis, programming) and the systems inside of the vehicle (system functions).

A further primary task of the vehicle configuration management system is the query, cyclic or upon request, of the configuration of the currently installed control units, and to use this to generate an equipment installation table that represents the current status, SVT-current. A comparison between SVT-nominal and SVT-current then takes place in order to determine whether the configuration installed in the vehicle is the same as the configuration that the vehicle should have. A fault memory entry is saved in the VCM if this reveals any discrepancies.

Additionally, upon request the vehicle configuration management system generates lists of control units that have specific characteristics.

Finally, the vehicle configuration management system has the task of determining those control units that have different serial numbers since a reference time (writing of SVT nominal).

The Service Department can use this to determine those control units that have been replaced since this time.

After replacement or changes to hardware or software, for instance, it is much easier to reestablish a consistent and working status for the vehicle electrical and bus systems.

Furthermore, the required configuration must not be maintained by each system function itself. This produces savings in component development as well as in system integration and logistics as compared to previous systems. Additionally, faults due to inconsistent configuration information are prevented.

Deviations from the specified configuration (SVT-nominal) and the current configuration (SVT-current) queried by the control units are identified.

## Data Storage

The vehicle configuration management system provides detailed information on the hardware and software installation status of the vehicle. To the outside, the VCM makes available that, and only that, which is relevant for its users. Direct access to internal structures is prohibited and is instead achieved via defined interfaces.

The vehicle configuration management system administers the following data for all electrical components in the vehicle:

- Specified equipment installation table (SVT-nominal)
- Vehicle order (FA)
- Vehicle profile (FP) and
- I-levels

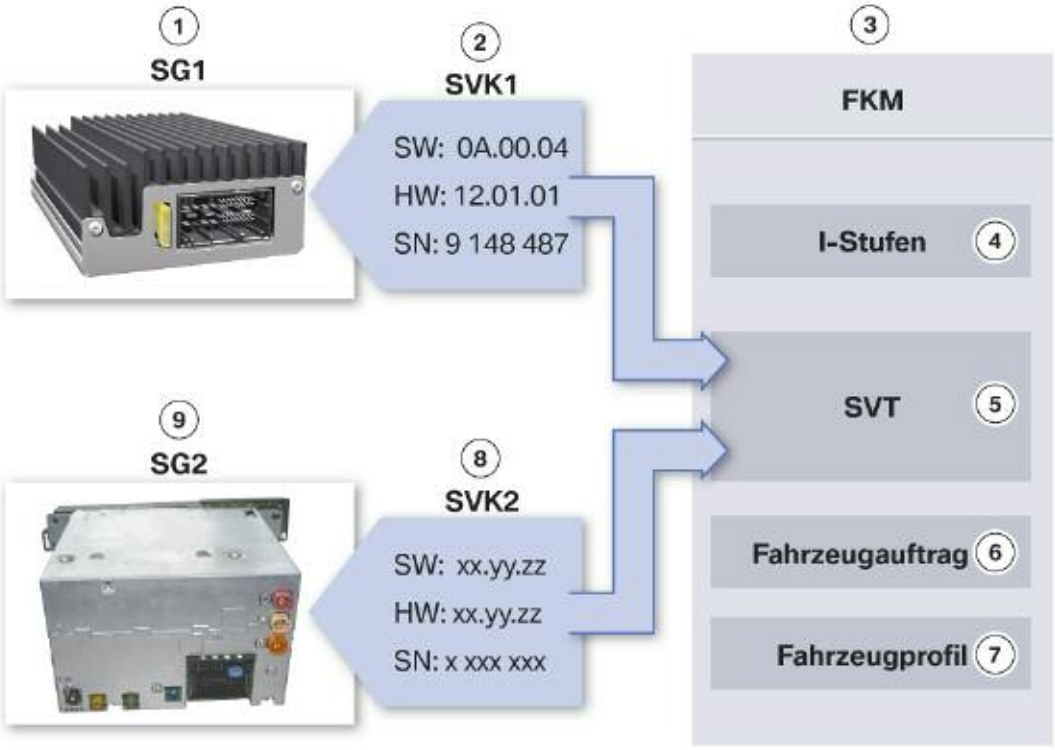
**Equipment Installation Table (SVT)**
The equipment installation table (SVT) contains all equipment installation identification lists (SVK) of all users installed in the vehicle electrical and bus systems.

The equipment installation identification list (SVK) is a list of all components (software and hardware). The component is not to be confused with the control unit as a control unit may be made up of several units. For instance, a CCC comprises several software units such as: user interface (BO), antennas (ANT), audio system controller (ASK), gateway (GW) as well as the hardware unit.

The vehicle configuration management system checks the current configuration 10 seconds after the engine start. This creates the current-equipment installation table. The nominal configuration (SVT nominal) is also saved in the vehicle configuration management system. If discrepancies are determined between SVT current and SVT-nominal a fault memory entry is saved in the ZGM.

New nominal values are written into the VCM during vehicle programming and coding.

**Storage of data by the vehicle configuration management system**



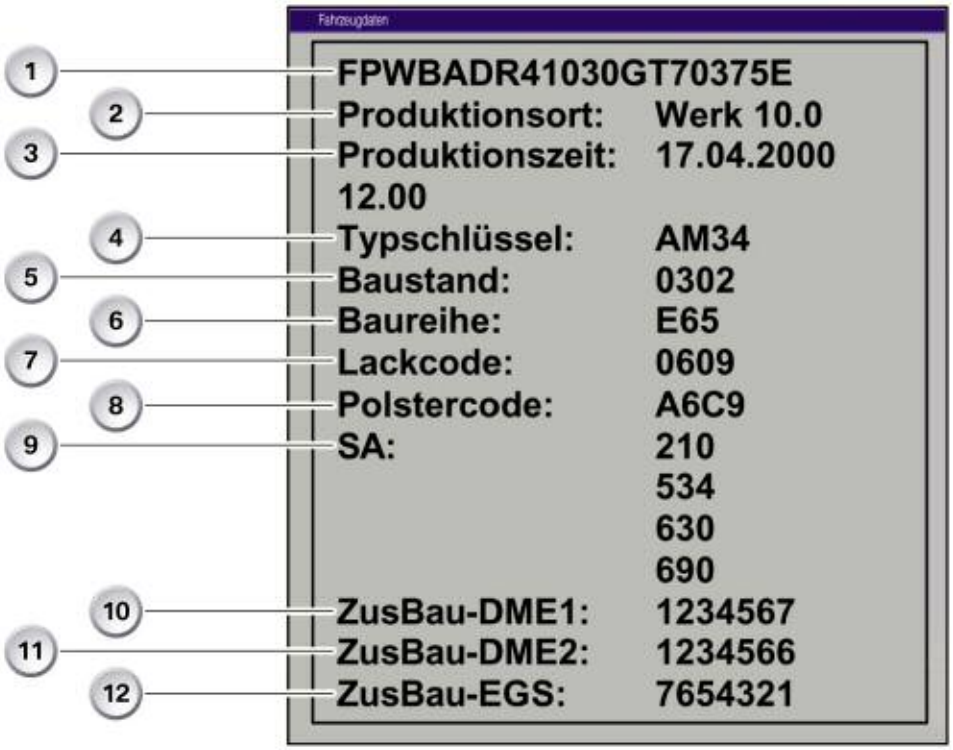

| Index | Explanation |
|---|---|
| 1 | Control unit 1 |
| 2 | Equipment installation identification list 1 (SVK1) |
| 3 | Data structure in the vehicle configuration management system |
| 4 | I-levels |
| 5 | Equipment installation table (SVT) |
| 6 | Vehicle order (FA) |
| 7 | Vehicle profile (FP) |
| 8 | Equipment installation identification list 2 (SVK2) |
| 9 | Control unit 2 |

## Vehicle Order

The vehicle order contains all the important equipment features of the vehicle in addition to the type code.

The assembly numbers of the drive control units are stored in the vehicle during assembly and can no longer be changed. It is therefore possible at any time to identify which part numbers of the control units were allocated to the vehicle during production.

**Vehicle order data**




| Index | Explanation | Index | Explanation |
|---|---|---|---|
| 1 | Vehicle identification number | 7 | Paint code |
| 2 | Production location | 8 | Upholstery code |
| 3 | Production time | 9 | Options (SA) |
| 4 | Type code | 10 | Assembly number DME-1 |
| 5 | Build date | 11 | Assembly number DME-2 |
| 6 | Model series | 12 | Assembly number 7654321 |

## Vehicle Profile

The vehicle profile contains additional data that precisely describe the vehicle. In addition to the development model series and design they include, for instance, the gearbox type, engine, version etc.

**Vehicle order data**


| Index | Explanation | Index | Explanation |
|---|---|---|---|
| 1 | Vehicle profile | 8 | Fuel |
| 2 | Development model series | 9 | Performance class |
| 3 | Battery class | 10 | Emgine |
| 4 | Design, e.g. Saloon | 11 | Gearbox type |
| 5 | National-market version | 12 | Number of cylinders |
| 6 | Steering side | 13 | Cubic capacity |
| 7 | Optional extra (SA) | 14 | Version |

## Initialization of the Vehicle Configuration Management System

Initialization of the VCM means the first writing of data. All data (SVT-nominal, vehicle order, vehicle profile and the I-levels) is written into the central gateway module through the initialization.

Initialization takes place in the factory and must always be performed when the ZGM is replaced.

Initialization is automatically performed by the programming system. Data from the vehicle order (FA) and I-levels on security are always stored in the CAS. The programming system firstly collects these data from the CAS and then writes them into the ZGM.

**Reading and Writing of Data**
The SVT-current, SVT-nominal, vehicle order, vehicle profile and the I-levels can be read out from the VCM via diagnosis. These data are written in the VCM during vehicle programming and coding. SVT nominal, FA, FP and I-levels can be written independently of each other.

For data security reasons, signatures are used in the data exchange between the diagnosis or programming systems and the VCM.

## Example of Vehicle Configuration Management

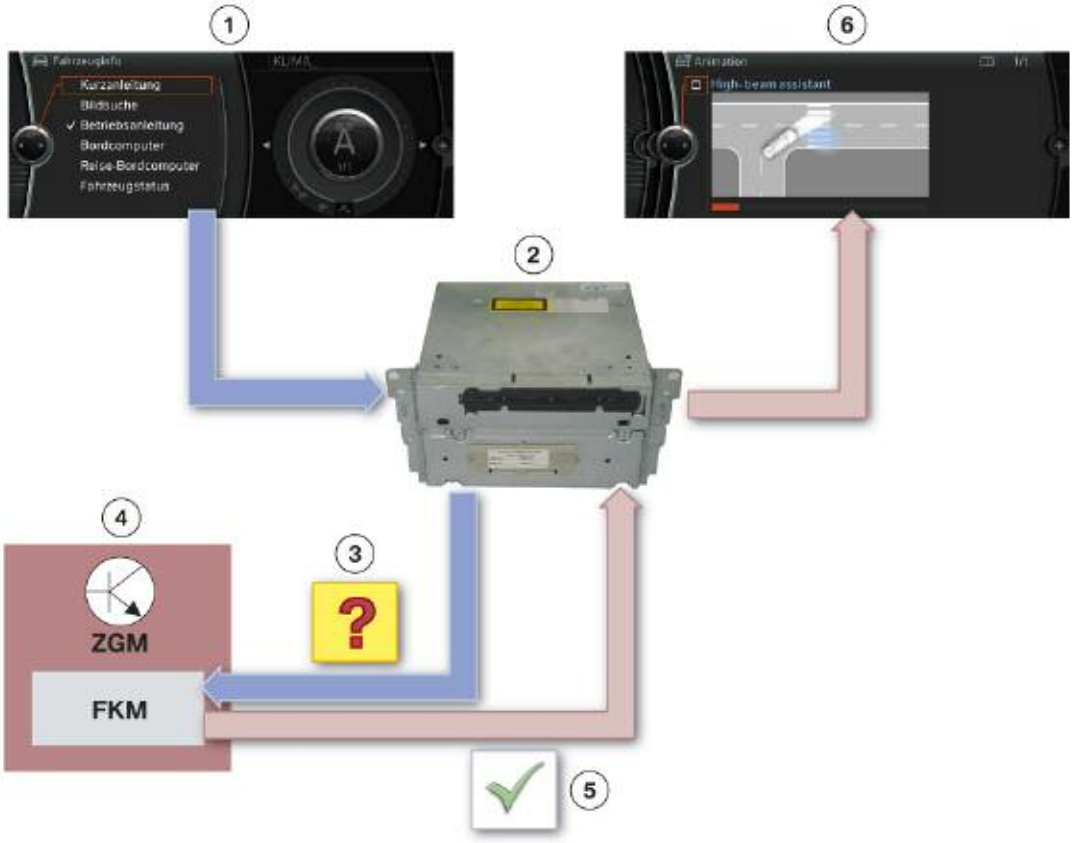
Upon request by other system functions (e.g. integrated Owner's Handbook), the VCM extracts a control units list, e.g. a list of all installed control units, from the SVT-current.

All the contents of the integrated Owner's Handbook are stored in the CIC, but only the vehicle-specific contents are shown. For instance, the CIC queries whether the high beam assistant is installed. If it is, the contents on the high-beam assistant are shown (graphic illustration on the next page).

Further system functions that revert to information from the VCM are, for instance:

- Personal profile (needs information on changes to the vehicle configuration).
- Diagnostics Master (needs list of the actively signalling control units).

## Query to VCM on installed control units




| Index | Explanation |
|---|---|
| 1 | Integrated Owner's Handbook is called up |
| 2 | CIC (queries the VCM on installed control units and makes vehicle-specific contents available) |
| 3 | Query to the VCM on installed control units e.g. high-beam assistant or KAFAS |
| 4 | VCM in the ZGM gives information on installed control units |
| 5 | The high-beam assistant or KAFAS is installed in this vehicle |
| 6 | The appropriate notes on this topic are shown in the CID |

# SWEEPING Technologies

SWEEPING technologies allows protection against copying, usage and manipulation of IT components and their software.

The abbreviation SWEEPING stands for **S**oft**w**are **E**nabled **E**lectronics **P**latform for **I**nnovative **N**ext **G**eneration Technologies.


SWT is based upon an encryption process that uses a key specific to a vehicle and control unit, the activation code as it is called, to activate a software function or application for a control unit.

The activation code (Freischaltcodes - FSC) is input in the Service Department or by the customer.

This occurs either by an input in the controller or through the import from CD/DVD or USB stick as an import medium for the BMW programming system.

The activation code is then subsequently input in the respective vehicle via the BMW programming system.

The required software is operable only after input of the activation code.

## Activation by Means of Activation Code

### Introduction of SWT Hardware Activation

The first activation code for a BMW vehicle was used in March 2006 for activation of the night vision camera following a replacement.

The hardware component was activated and therefore made operable.

A legal requirement was the background for this. Strict conditions applied for the night vision camera that was developed especially for military purposes.

They could only be installed in registered vehicles. This allowed the vehicles with SA 611 (night vision) to be recorded and accounted for in strict conformity with license conditions.

Furthermore, usage of a FSC allowed clear allocation of the hardware component (night vision camera) to the vehicle in which it was installed.

An activation code for the night vision camera following a replacement was enclosed in the form of a CD. This so-called "subpart" had to be ordered by the parts technician over the EPC by giving the vehicle identification number.

The activation code located on the CD was requested by the BMW programming system during the programming. It was then transferred into the BMW programming system and imported into the vehicle.

If a FSC was not entered during programming or coding, it was not possible to activate BMW Night Vision. This was displayed after programming/coding by a Check Control message in the instrument panel.

**Introduction of SWT Software Activation**
In March 2007 the activation of single software components was commenced at BMW. This laid the foundation stone for the business model "software as a product".

It allowed functions already installed in the vehicle to be made usable for the customer and to activate them by means of an activation code.

This in turn created the opportunity to invoice software licenses individually with the supplier and only after its activation. In addition, copy protection was hugely improved by activation code activation, an asynchronous encryption method.

**Activation of the Voice Recognition System in the CCC:**
An activation code for the voice recognition system (SA 620) in connection with CCC (SA 609) became necessary when programming a vehicle from Progman V25.0, as the voice recognition system could no longer be used without this.

This applied for the retrofit of software for the voice recognition system as well as for replacement of the CCC.

Savings in license costs was the background, as invoicing could now be carried out with the software manufacturer separately for each vehicle instead of a general license.

When programming of the CCC (SA 609) was carried out on vehicles up to March 2007 fitted with the voice recognition system (SA 620) or voice recognition system preparation (SA 6UB), the BMW Programming system requested an activation code.

This activation code was located on a separate DVD or in the ASAP portal (only available in the ASAP portal after prior completion of an order).

On vehicles with a production date from March 2007 (I-level 07-03-5XX or higher) the activation code was contained in the CCC.

In the event of a hardware replacement for the CCC however, it is not possible to import the code from the SWT disc. The data does not exist on the CD.

The necessary code has to be ordered together with the replacement module via EPC and will be delivered via the ASAP portal (see page 126).

**Note: Vehicles produced from 3/2007 require an activation code acquired from the ASAP portal.**

## SWEEPING Technologies in the F01/F02

From the F01/F02 the activation of software applications and function has been increasingly expanded.

It is now possible to activate the following applications or software functions via FSC:

- Software for voice recognition (SA 620)
- Navigation system application software (SA 609)
- Navigation system map data (activation code required from the second half of 2009)

The activation code for the software applications and software functions named above is loaded over the BMW programming system into the vehicle in nearly all cases. The CD is still necessary for activation of the camera for the night vision camera following a replacement.


**Navigation system map data**

## Update of map data for the navigation system and input of the activation code

Since 09/2008 with introduction of the Car Information Computer, the navigation system map data is stored on a hard disk in the CIC.

Input of the map data is currently possible from the DVD drive and in later production vehicles over the programming system.

The activation code can also be entered over the programming system or via the controller of the iDrive system. An input aid (speller) is available in the iDrive display for this purpose.

This activation code along with the current navigation software (Navigation DVD) is handed to the customer when the customer purchases the map update.

When the order is placed for the activation code, the parts technician states the vehicle identification number of the vehicle for which the navigation map is to be updated.

A special activation code is consequently created in the BMW AG headquarters, in which the vehicle identification number becomes an element of the FSC.

This means the issued FSC and navigation DVD can only be used for the vehicle requested.

The initial filling of the hard disk integrated in the CIC with map data can, if this manufacturer has not already filled it, only be carried out over the BMW programming system.

For the update of map data, only the cash sale variant with activation code input via the speller is subsequently available.

**Delivery Process of the Activation Codes Over ASAP**
The majority of software functions and applications are not activated by customers, rather by BMW Service employees over the BMW programming system.

A special process was created for BMW employees to request the activation code from the BMW AG headquarters, to download it to the workshop PC and then to import it into the corresponding vehicle over the BMW programming system.

The part number for the activation code is available after input of the vehicle identification number in the EPC (Electronic Parts Catalog).

Upon request from the BMW Service employee, the parts technician orders the activation code over the appropriate Dealer Management System.

The activation code is now created in the BMW AG headquarters. It is normally available to the Service employee in the ASAP portal within a very short time.

**Note: The delivery time for the activation code may be delayed for up to one workday due to country-specific circumstances and the world-wide time difference.**

The activation code is now ready for download as a ZIP folder (content = 3 files) in the ASAP portal and is shown after input of the corresponding vehicle identification number.

This ZIP folder must be saved in a temporary directory for subsequent extraction of the contents.

These "unzipped" contents are now to be saved in on a CD/DVD or via the use of a USB stick as long as it has been formatted as a removable disc.

**Note: No external USB hard drives will be supported.
Not all USB devices are compatible with the system.**

**Note: Cancellation of the activation code is only possible before the start of the download. Therefore, a check should be made before the download of whether the vehicle identification number of the customer's vehicle is correct. The activation code is invoiced when the download starts even though it has not been installed in the customer's vehicle.
Cancellation after the download is therefore no longer possible.**

## Input of the Activation Code into the BMW Programming System

The medium containing the three unzipped files is inserted into the ISSS so that the BMW programming system can access these FSC data.

After the import button has been pressed, follow the on screen instructions to complete the import process.

**ISSS**

**Import of the activation code into the BMW programming system**

## Planned Expansion Stages

In the expansion stage of the BMW programming system planned for the future, the data import of the activation code is to happen automatically.

This would mean that after the request by the parts technician, the activation code, would be directly available to the BMW programming system after a short waiting time.

This process, called "SWT-Online", plays an important role particularly for repairs. Because after replacement of a Car Information Computer, for instance, work can be carried out on a repair without an activation code having to be ordered. It is made directly available to the BMW programming system by "SWT-Online".

However, it is still necessary to place an order over the parts technician and the Dealer Management System for software that has to be paid for, such as the voice input system.

"SWT-Online" or the ASAP portal can be selected afterwards as the delivery channel.

Cancellation of the activation code is however only possible over the ASAP portal.

The channel over the ASAP portal, with download onto the workshop PC and subsequent import into the BMW programming system, should therefore continue to be used as the backup-solution.

Should problems occur during the download or data import into the vehicle, technical support of the respective market should be contacted or a PuMA instance created.

# Vehicle Security

## History and Fundamentals

Vehicle security protects the vehicle electrical and bus systems against unauthorized manipulative external access.

The topic of vehicle security experienced its beginnings with the introduction of the E28.

On this 5 Series, an instrument panel with encoding connector (coding plug) was installed from 1980.

When a new instrument panel was installed, the encoding connector of the old one had to be used. If this was not done a manipulation dot lit up to indicate that the kilometer reading had been manipulated.

The kilometer reading was only reset to the correct reading with the old encoding connector. The manipulation dot was no longer displayed.

A new era in manipulation protection begins with introduction of the master security module (MSM) as a module in the central gateway module in the F01/F02 and the client security module (CSM) in some selected control units.

The basis for the requirement for the vehicle security system is formed by the growing amount of electronics and the interlinked networking installed in the vehicle.

Mention must also be made of the increase in driver-based services.

**Threat Potential**
As electronics increase in vehicles, the possibilities also increase of disrupting and infiltrating this sensitive system through manipulation, imitation of hardware and software, and tuning measures (blackbox tuning).

Data storage in the vehicle (e.g. Contacts menu) also means that adequate data protection must be provided.

## Vehicle Security Measures

The measures below are carried out to be able to ensure vehicle security in the F01/F02:

- Periodic check of software signatures (signature = digital, electronic signature used for checking the completeness, genuineness and intactness of data)
- Individual stamping of control units on the vehicle in which they have been installed
- Cryptographic protection of the teleservice access
- Encryption of personal data
- Periodic checking of memory ranges.

## Benefits for Customers

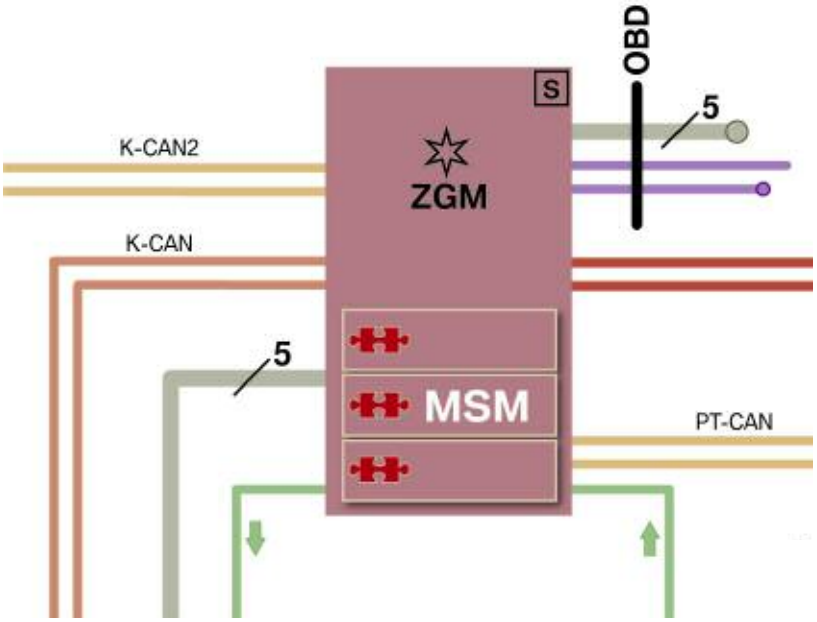
The vehicle security system actively protects the personal data of the customer and actively guards the vehicle electrical and bus systems against attempted manipulation from outside.

## Benefits of the Vehicle Security System for the BMW Group and the BMW Brand

For the BMW Group, the vehicle security system contributes towards unjustified liability and to warranty costs not being accrued for manipulation.

Furthermore, vehicle security has the purpose of preventing vehicles damaged by manipulation giving a bad public image to the BMW brand and therefore damage to our reputation.

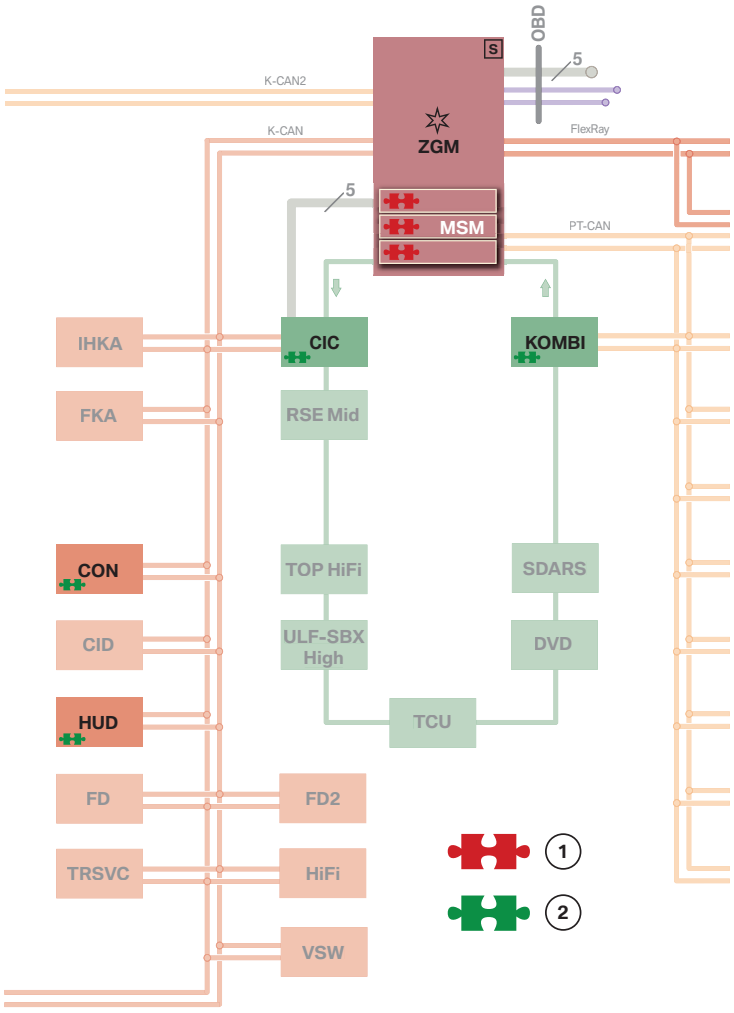
**Master security module in the ZGM of the F01/F02**



Secondly, the vehicle security system comprises the client security modules located in the control units below that are monitored by the master security module:

- CIC - Car Information Computer
- KOMBI - Instrument Cluster
- HUD - Head-up Display
- CON - Controller

**Overview of the MSM and the individual client security modules**




| Index | Explanation |
|---|---|
| 1 | Master security module in the central gateway module |
| 2 | Client security module in the individual control units |

## Vehicle Security Operating Principle

The master security module periodically transmits queries to the individual client security modules.

Any faults and discrepancies are documented and notified to the BMW AG headquarters during transmission of the FASTA data via Jetstream during a service visit.

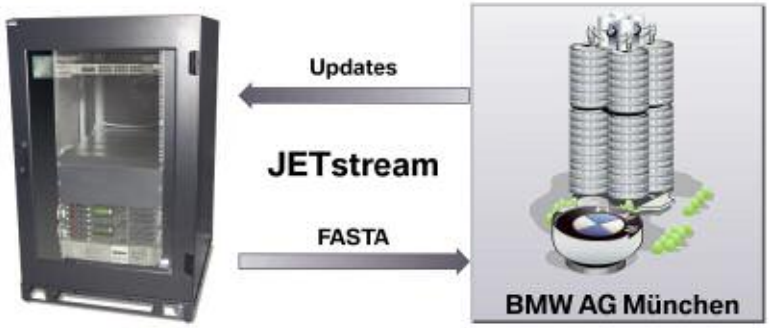
It is not possible for Service Department employees to use BMW diagnosis systems for accessing the information regarding manipulation stored in the control unit.

Possible faults and discrepancies in the vehicle security system are:

- A control unit was replaced without authority.
- A control unit was manipulated through a change of software or data status.
- Communication to the MSM was interrupted or manipulated for a control unit with a CSM.

## Preservation of Function in the Vehicle Security System

Any manipulation found in the vehicle security system must not have a negative impact of functions relevant for security within the vehicle electrical and bus systems.




**Data transmission via JETstream**